An Integrated Total S&MA Management Framework

-Introducing the Triple-Triplets Concept for Risk-informed Comprehensive S&MA Management

Feng Hsu, Ph.D.

Feng.Hsu@JSC.NASA.GOV

Sr. Staff at SAIC, NASA JSC/NC62, Shuttle Safety & Mission Assurance

Houston, TX 77058

Presented to NASA RMC V & PRAXI 5

NASA Risk Management Conference – RMC-V 2004

NASA Assurance Technology Center, Cleveland, Ohio

October 27-29, 2004

Space Shuttle Program

F. Hsu

NASA

Why An Integrated Total S&MA Management Framework Is Important?

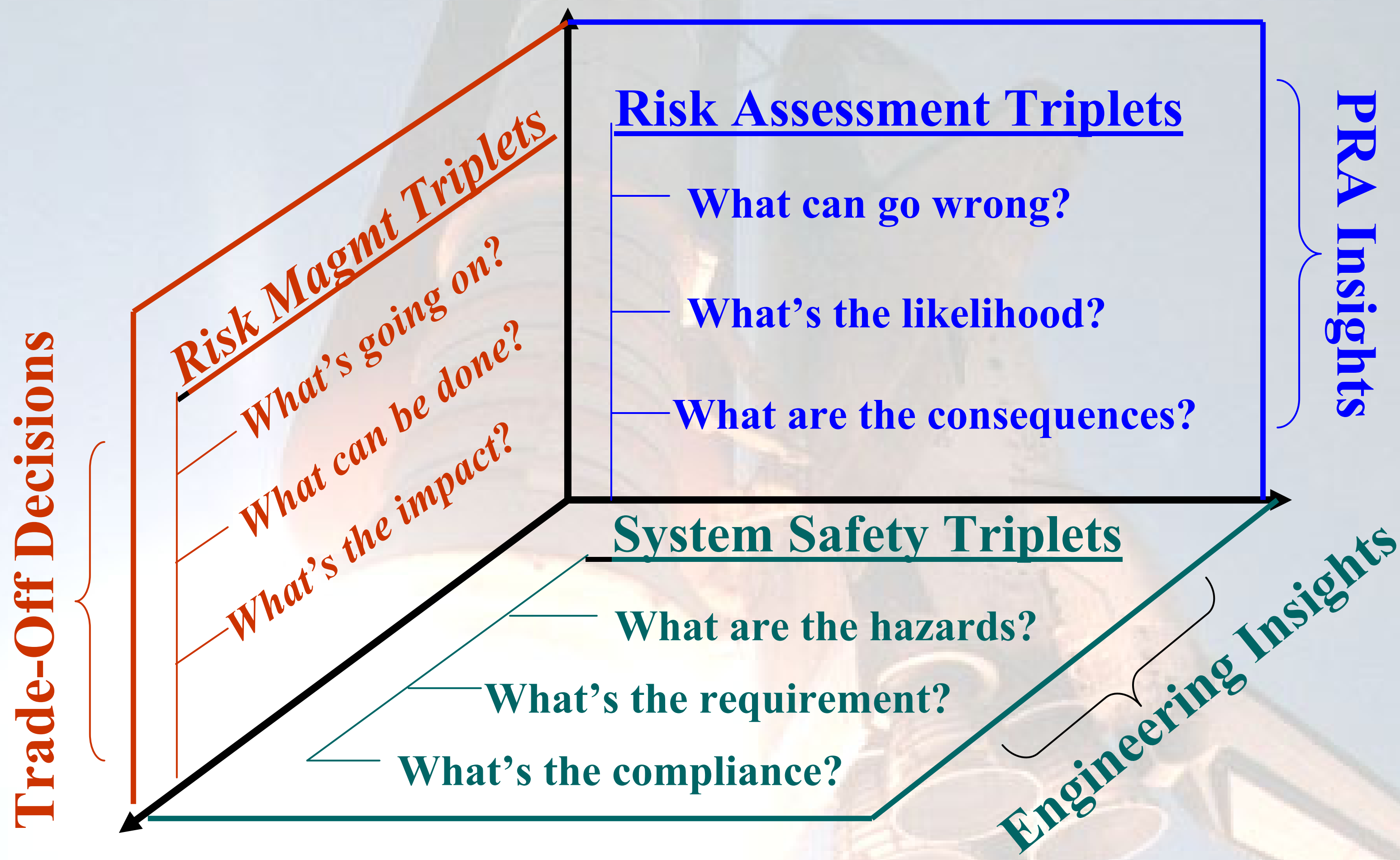
- A resolution to S&MA issues as pointed out in the CAIB report:
  - "Risk information and data from hazard analysis are not communicated effectively to the risk assessment and mission assurance process …"
  - "System safety engineering and management is separated from mainstream engineering …."
  - "Over the last two decades, little to no progress has been made toward attaining integrated, independent, and detailed analysis of risk …."
  - No process addresses the need to update hazard analysis when anomalies occur."
  - Need of "a disciplined, systematic approach to identifying, analyzing, and controlling hazards …"
- The complexity of STS and its successful operation necessitates an integrated total S&MA management process
- Hazard, Risk and Safety are integral elements to comprehensive S&MA management of any complex engineered systems.
- Need of An Integrated Process for Combining Hazard Analysis with PRA for Total Safety and Risk Management (can't be separated!)
- Utilization of A Systems Engineering Approach (closed loop system)

Why An Integrated Total S&MA Management Framework Is Important? (Cont'd)

- **The New Reality & Challenges for NASA**
  - **Fundamentally new**
  - **Greater Complexity**
  - **Multifaceted**
  - **Public Scrutiny**
  - **Uncertainty**

F. Hsu

A Triple-Triplets (“Double T”) Concept for An Integrated S&MA Management Framework



Why a Triple-Triplets (Double-T) Concept is Needed?

Conceptual Differences of System Hazard, Risk, Safety, Reliability:

HAZARD - System threat existed that can cause potential damage & harm. A necessary condition for risk but not absolute condition for risk or damages.

RISK - A integrated measurement of consequence of a undesired event occurrence. Not necessarily a mathematically measurable quantity

SAFETY - Assurance or level of confidence in accident/damage prevention & control. The system safety concept is the application of systems engineering and mgmt to the process of hazard, safety & risk analysis to identify, assess & control associated hazards while designing or modifying systems, products, or services.

RELIABILITY - Assurances of expected proper functioning of equipment, systems, hardware or software component as well as human performances etc. Low reliability must induce high risk but low risk not necessarily come from high reliability.

F. Hsu

The System Safety Triplets

- A Safety Engineering Process

1. **What are the hazards?**

   Failure source identifications **(hardware/software/human/organization/external)**

   Hazard analysis/Hazard ranking using risk index matrix (semi-quantitative FTA)

   FMEA/FMECA and CILs on root cause identification & initiator ranking

2. **What are the safety requirements & goals?**

   Develop safety requirements & goal - when & where to impose?

   What are the organizational hierarchy & assurance for hazard control?

   Process for ensuring reliability, maintainability, supportability & inspections

3. **What's the compliances & verification?**

   Safety audit & regulatory mechanisms **for compliance & verifications**

   Process for documentation control and hazard/risk communications

   Culture for two-dimensional (vertical/horizontal) Risk/Hazard communications

The Risk Assessment Triplets

- A PRA Process To Gain Risk Insights

1. **What can go wrong?**

   Risk identification **(for all credible & significant hazards)**

   Hazards & Initiating event identification

   Scenario development, enumeration and structuring

2. **What's the likelihood that it would go wrong?**

   Risk quantification & measurement

   Reliability & Data assessment

   Risk evaluation & uncertainty assessment

   Risk ranking & importance measures

3. **What are the consequences?**

   Risk mitigation & Damage assessment

   Failure & success criteria evaluations

The Risk Management Triplets

- A Risk-Informed Decision Process

1. **What's going on?**

   Trend Analysis **RM & Risk-based performance monitoring/evaluation**
   Indicator technology - quantitative/qualitative trend/time series assessment)
   Accident Sequence Precursor (ASP) identification & evaluations
   Data mining & statistical anomalies/near-miss assessment
   Communication of issues & problems

2. **What can be done?**

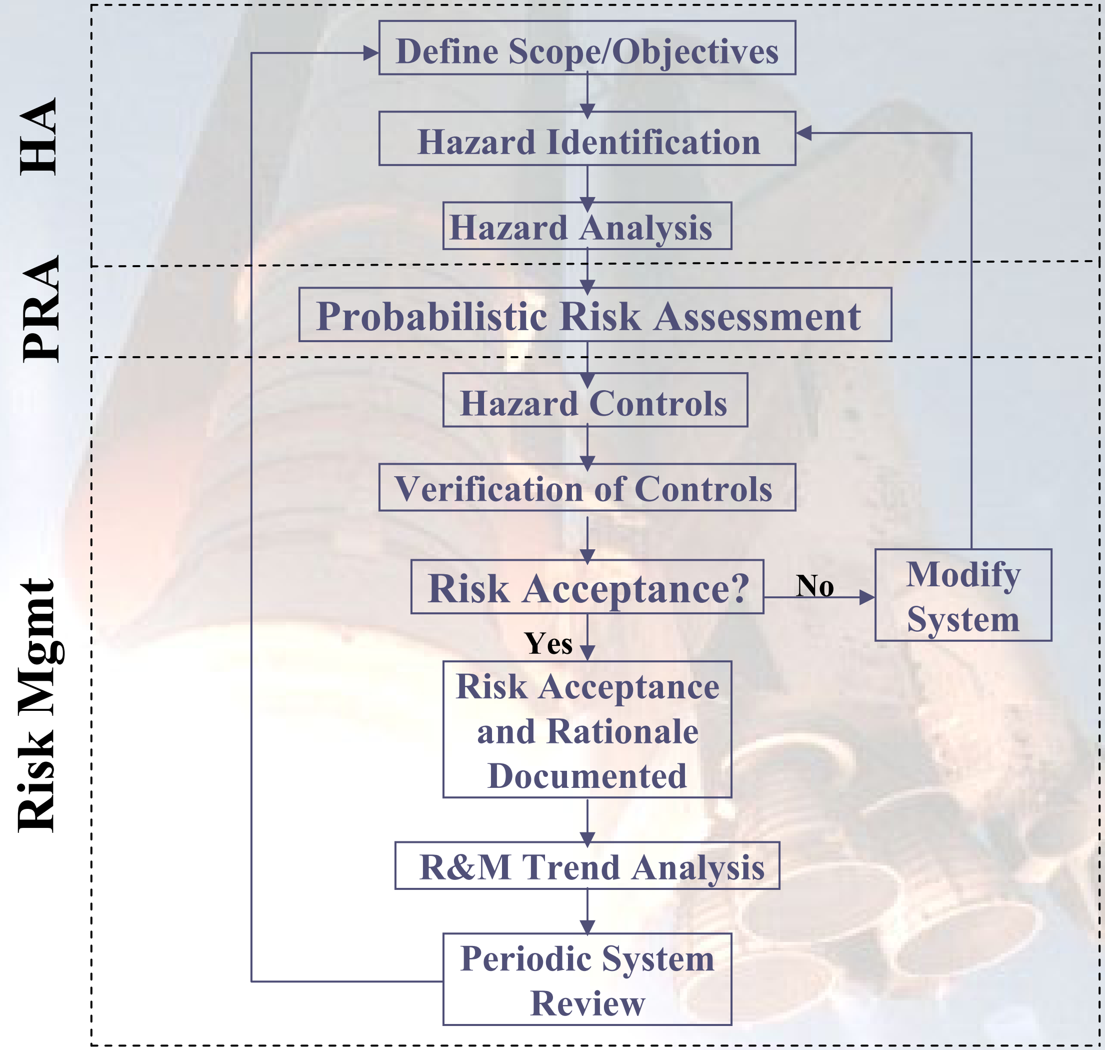
   Trade-off studies **using insights from both PRA & Hazard Analysis (HA)**
   What options are available & what are their associated trade-offs?
   Multi-objective, optimized cost-benefit analysis (CBA) & decision making

3. **What's the impact?**

   Impact assessment **of current mgmt decisions on future options (risk reduction)**
   Impact of risk control evaluations of risk mgmt activities on safety improvement

The "Double-T" S&MA Management Concept

A Simplified Example Systems Engineering Process

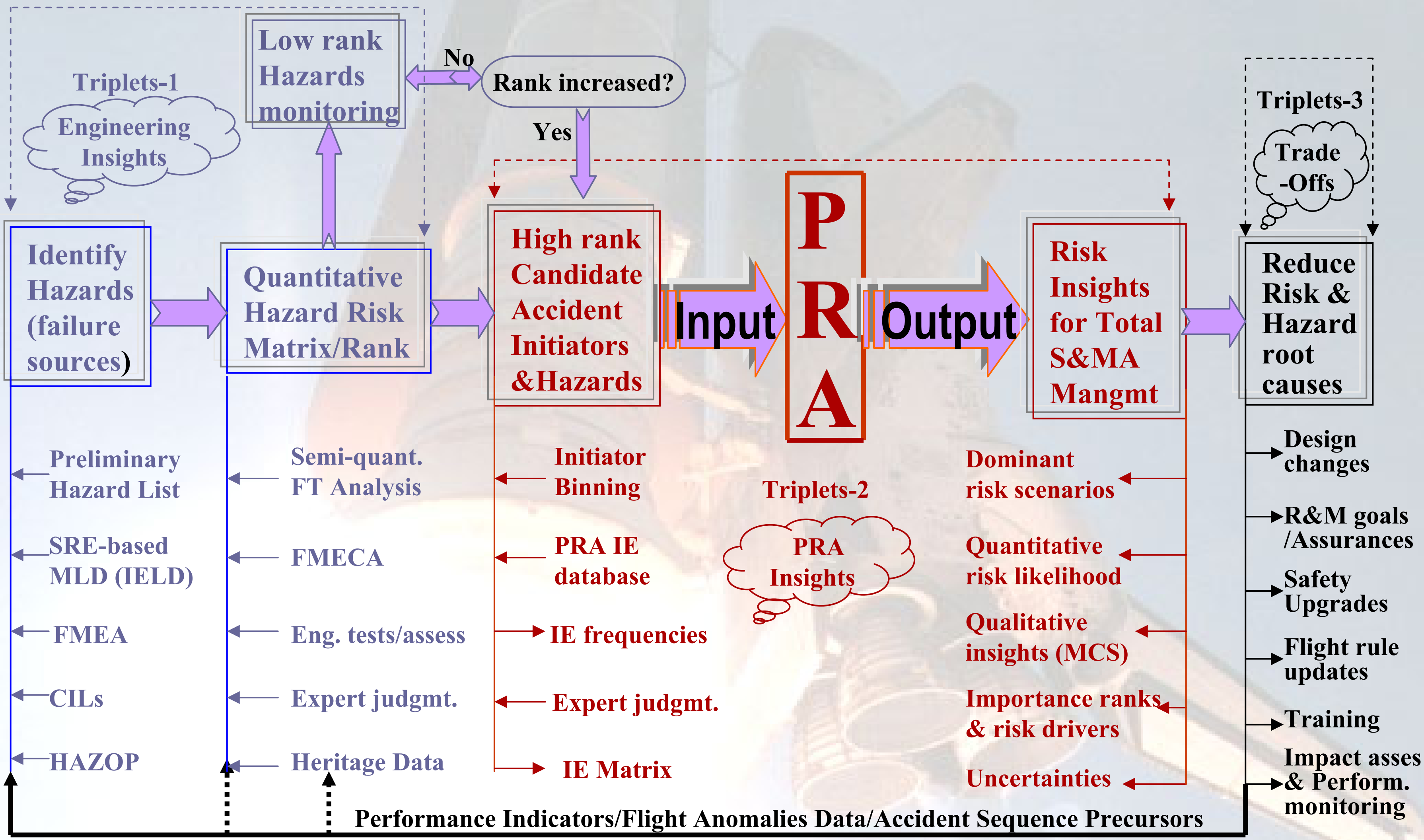


Space Shuttle Program

F. Hsu

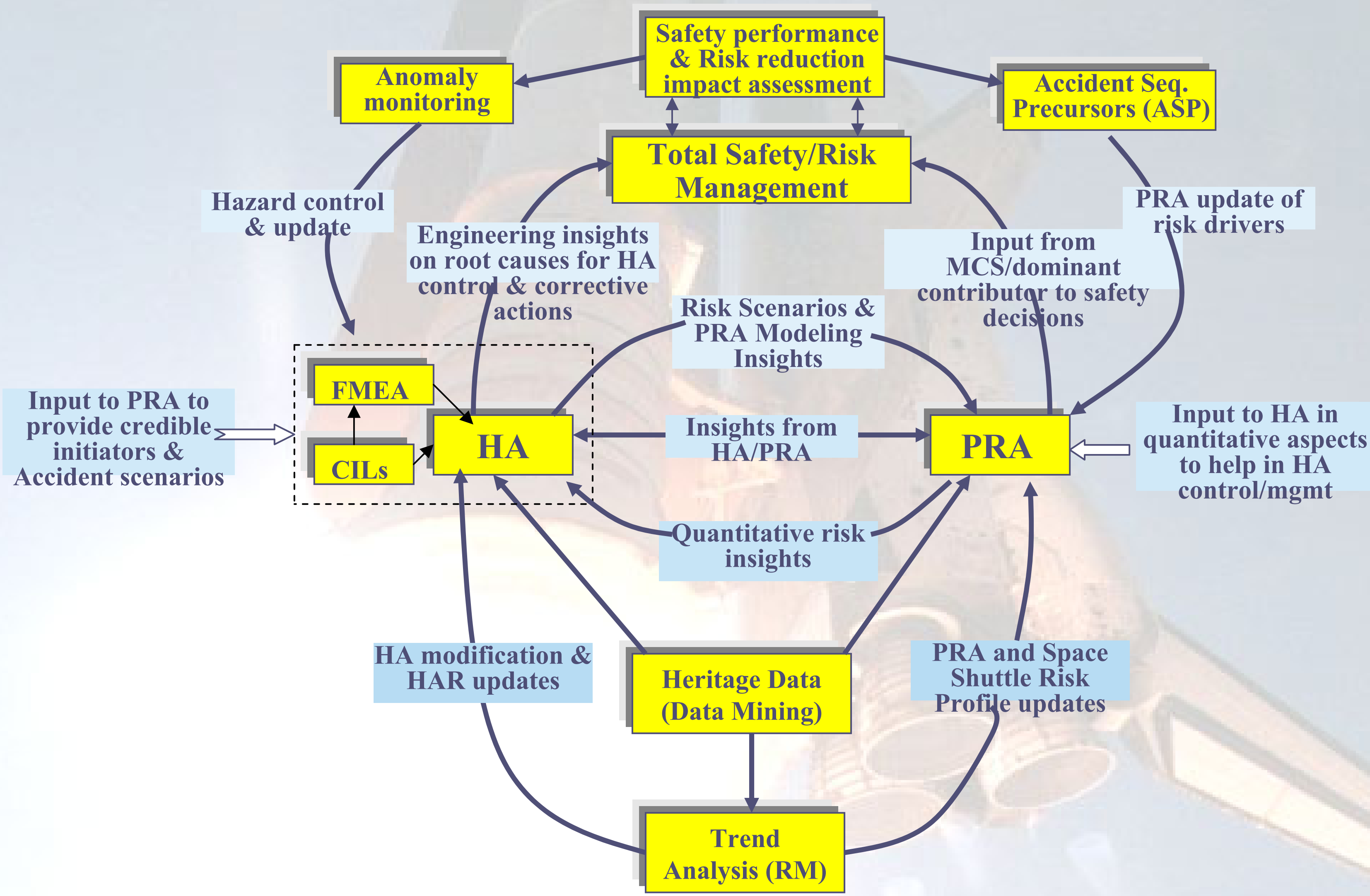
The "Double-T" S&MA Management Framework

- Role of HA & PRA in the "Double-T" S&MA Mgmt Process



The "Double-T" S&MA Management Framework (Cont'd)

- An Integrated Process for Combining Hazard Analysis with PRA for Total Safety and Risk Management



The "Double-T" S&MA Management Framework – Key Elements

A Systematic & Comprehensive Approach for Hazard Identification/Analysis

A systematic accident initiator identification using SRE (Scenario-structured Risk Envelope) concept

A method to combine & incorporate Hazard Analysis (HA) process into PRA

A Systematic HA Approach which ensures completeness in searching, analyzing, ranking and reporting of hazard/failure sources for S&MA

A improved HA process, which becomes a key element of the proposed total Risk-informed S&MA management framework based on "Double T" concept

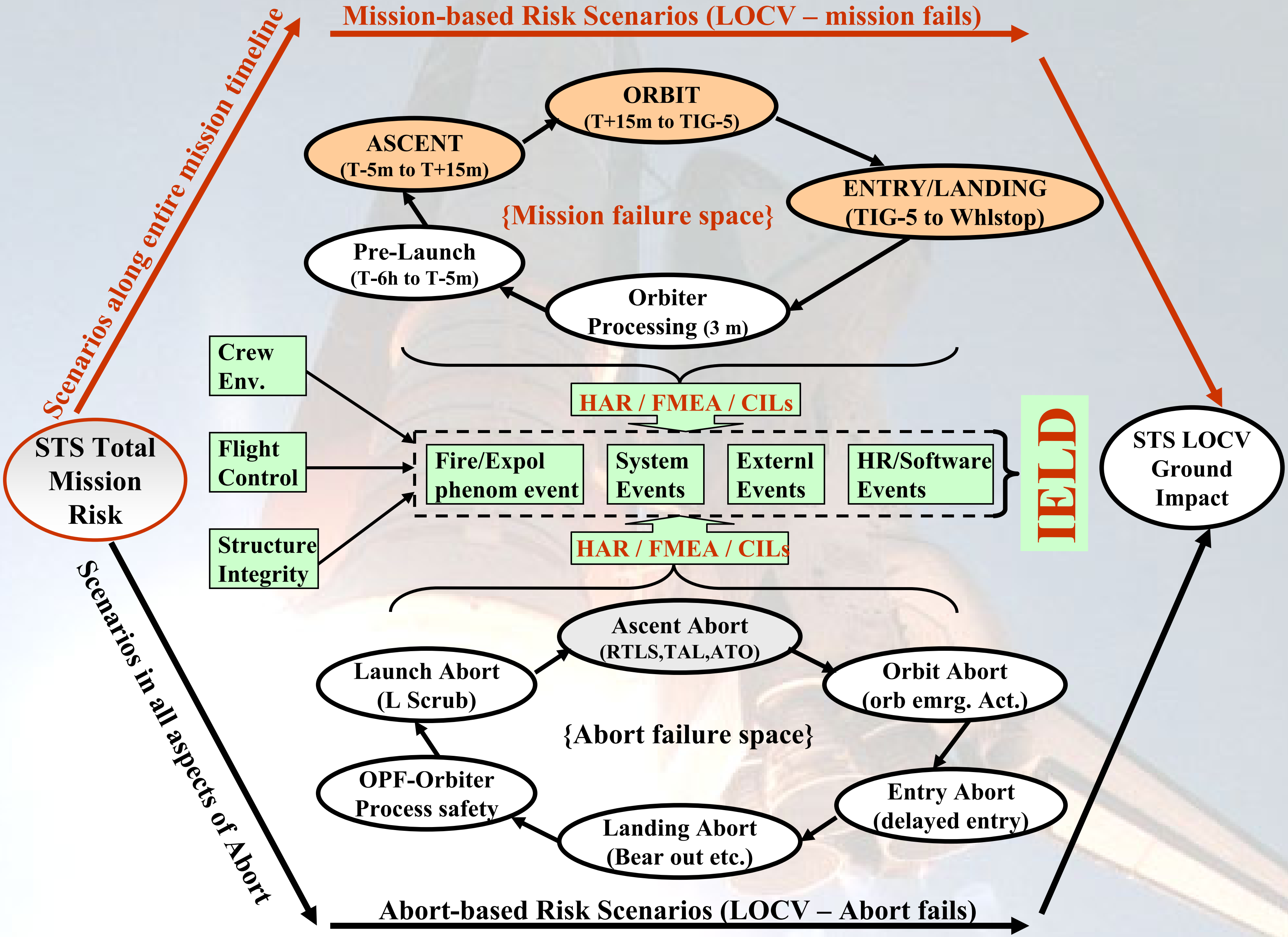
The "Double-T" S&MA Management Framework – Key Element (Cont'd)

- The Scenario-structured Risk Envelop (SRE) Concept for Searching & Identifying Hazards

  - The SRE adhere to the concept of "enveloping the risk" in completeness
  - The philosophy behind the SRE concept – finding accident before accident find us !
  - SRE – the need for completeness in PRA (all LOCV potentials are considered)
  - A systemic approach for searching candidate initiating events. searching the entire spectrum of all dimensions of failure space along phases, functions, and mission timeline

Illustration of the Scenario-structured Risk Envelop Concept

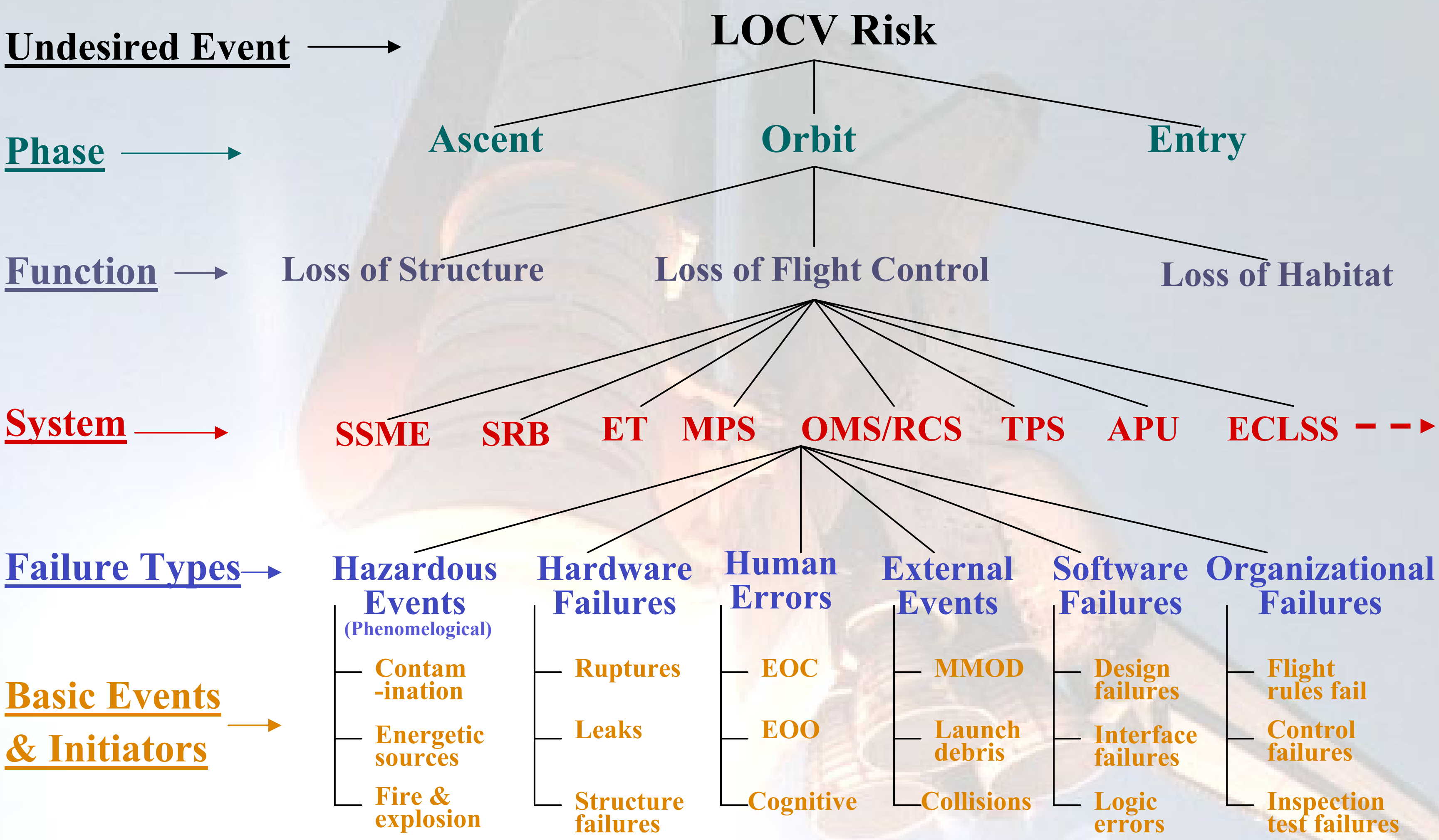
F. Hsu



The "Double-T" S&MA Management Framework – Key Element (Cont'd)

- The SRE-based Initiating Event Logic Diagram (IELD)
  - IELD - a matrix formed Initiating Event Logic Diagram. An effective tool for managing, documenting and representing vast amount of candidate hazardous initiating events for risk model considerations
  - A computerized IELD database format can be conveniently established
  - Similar to conventional MLD – Top down, summary logic diagram. It identifies and categorizes a more complete set of IEs.
  - SRE concept incorporates a functional thought process and provides a bridge to relate NASA's vast engineering assessment databank (HARs/FMEA/CILs)

An Example Hierarchy of SRE-based Initiating Event Logic Diagram (IELD) for Systematic Hazard Identification



Space Shuttle Program

F. Hsu

NASA

An Example Matrix-based Representation of IELD

The Matrix Representation of Modularized MLD Sub-trees for the Integrated Shuttle PRA $\{\text{MLD}\}_{7\times9}$

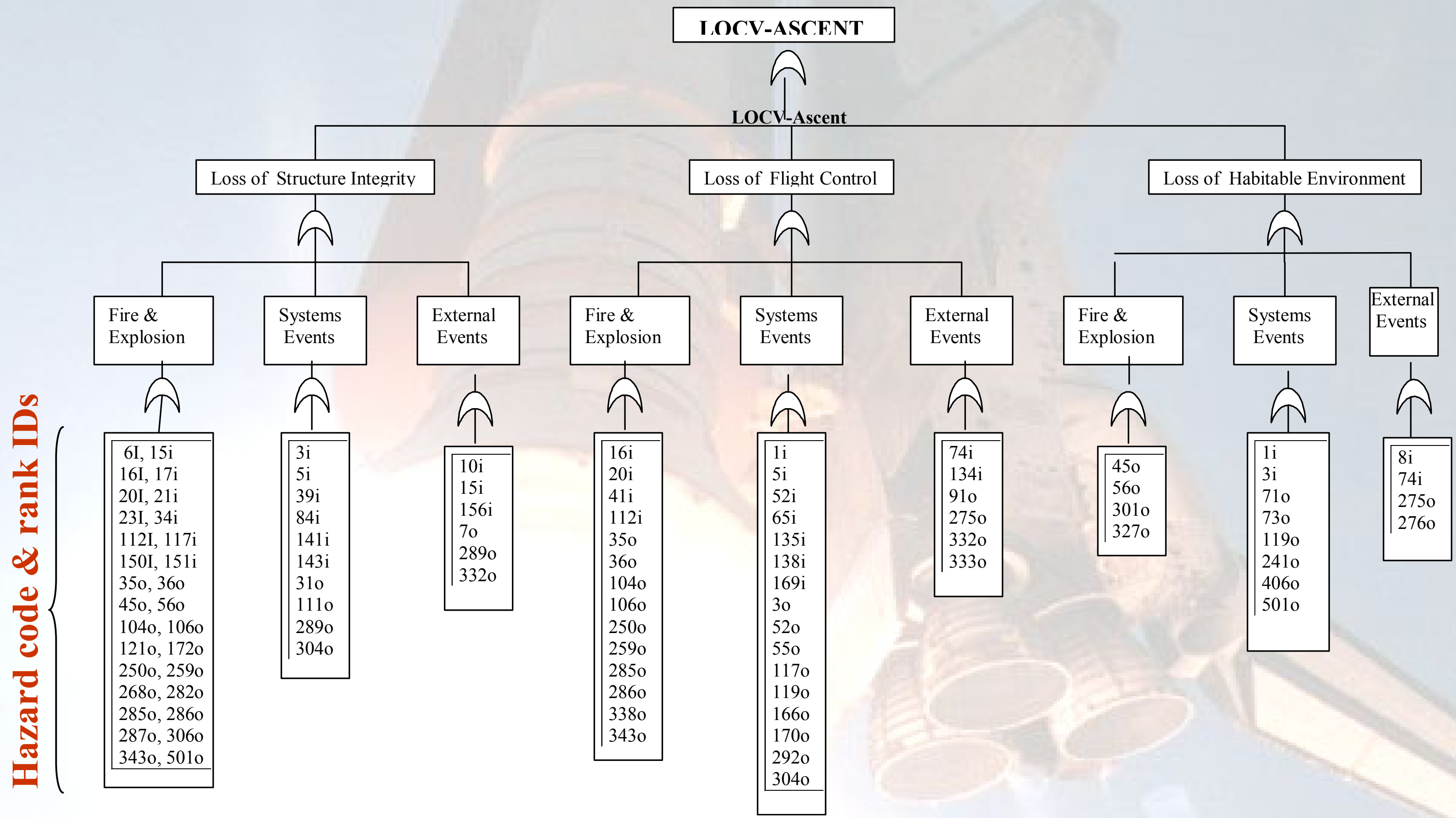
	Top-Level Func failures / Mission Phases	Loss of Structure Integrity			Loss of Flight Control			Loss of Habitable Environment		
		Fire/Explosion	Systems Events	External Events	Fire/Explosion	Systems Events	External Events	Fire/Explosion	Systems Events	External Events
Mission-Based Phases	1 LOCV-PreLch (LOCV During PreLaunch)	11 LOCV-PreLch-LS-FirExp	12 LOCV-PreLch-LS-SysEvt	13 LOCV-PreLch-LS-ExtEvt	14 LOCV-PreLch-FC-FirExp	15 LOCV-PreLch-FC-SysEvt	16 LOCV-PreLch-FC-ExtEvt	17 LOCV-PreLch-EN-FirExp	18 LOCV-PreLch-EN-SysEvt	19 LOCV-PreLch-EN-ExtEvt
	2 LOCV-Ascent (LOCV During Ascent)	21 LOCV-Ascent-LS-FirExp	22 LOCV-Ascent-LS-SysEvt	23 LOCV-Ascent-LS-ExtEvt	24 LOCV-Ascent-FC-FirExp	25 LOCV-Ascent-FC-SysEvt	26 LOCV-Ascent-FC-ExtEvt	27 LOCV-Ascent-EN-FirExp	28 LOCV-Ascent-EN-SysEvt	29 LOCV-Ascent-EN-ExtEvt
	3 LOCV-Orbit (LOCV During Orbit)	31 LOCV-Orbit-LS-FirExp	32 LOCV-Orbit-LS-SysEvt	33 LOCV-Orbit-LS-ExtEvt	34 LOCV-Orbit-FC-FirExp	35 LOCV-Orbit-FC-SysEvt	36 LOCV-Orbit-FC-ExtEvt	37 LOCV-Orbit-EN-FirExp	38 LOCV-Orbit-EN-SysEvt	39 LOCV-Orbit-EN-ExtEvt
	4 LOCV-DesLnd (LOCV During Des/Land)	41 LOCV-DesLnd-LS-FirExp	42 LOCV-DesLnd-LS-SysEvt	43 LOCV-DesLnd-LS-ExtEvt	44 LOCV-DesLnd-FC-FirExp	45 LOCV-DesLnd-FC-SysEvt	46 LOCV-DesLnd-FC-ExtEvt	47 LOCV-DesLnd-EN-FirExp	48 LOCV-DesLnd-EN-SysEvt	49 LOCV-DesLnd-EN-ExtEvt
Abort-Based Phases	5 LOCV-AbrtAsnt (LOCV During Asnt Abort)	51 LOCV-AbrtAsnt-LS-FirExp	52 LOCV-AbrtAsnt-LS-SysEvt	53 LOCV-AbrtAsnt-LS-ExtEvt	54 LOCV-AbrtAsnt-FC-FirExp	55 LOCV-AbrtAsnt-FC-SysEvt	56 LOCV-AbrtAsnt-FC-ExtEvt	57 LOCV-AbrtAsnt-EN-FirExp	58 LOCV-AbrtAsnt-EN-SysEvt	59 LOCV-AbrtAsnt-EN-ExtEvt
	6 LOCV-AbrtOrbt (LOCV During Orbit Abort)	61 LOCV-AbrtOrbt-LS-FirExp	62 LOCV-AbrtOrbt-LS-SysEvt	63 LOCV-AbrtOrbt-LS-ExtEvt	64 LOCV-AbrtOrbt-FC-FirExp	65 LOCV-AbrtOrbt-FC-SysEvt	66 LOCV-AbrtOrbt-FC-ExtEvt	67 LOCV-AbrtOrbt-EN-FirExp	68 LOCV-AbrtOrbt-EN-SysEvt	69 LOCV-AbrtOrbt-EN-ExtEvt
	7 LOCV-AbrtDeLd (LOCV During Descent & Landing Abort)	71 LOCV-AbrtDeLd-LS-FirExp	72 LOCV-AbrtDeLd-LS-SysEvt	73 LOCV-AbrtDeLd-LS-ExtEvt	74 LOCV-AbrtDeLd-FC-FirExp	75 LOCV-AbrtDeLd-FC-SysEvt	76 LOCV-AbrtDeLd-FC-ExtEvt	77 LOCV-AbrtDeLd-EN-FirExp	78 LOCV-AbrtDeLd-EN-SysEvt	79 LOCV-AbrtDeLd-EN-ExtEvt

F. Hsu

A Graphical Representation of IELD

A Graphical Representation of A Partial Initiating Logic Diagram (IELD)

(For ASCENT Phase of the Integrated Shuttle PRA)



List of Accident Initiating Events Identified in the IELD

(MPS Related Example Initiators)

USA Hazard Number	MLD initiating event	Mission Phase	System	PRA Consequence	Threatened Function			Hazard Category		Prob Category		Reference ESD Names	Analyst Remarks		Individual Hazard Description
								F/P	Type	Sev	Like		FT/ET	Justification	
INTG 006	4	PA	MPS	LOCV	SI			P	FE	A	c		FT		Ignition of Flammable Atmosphere at the ET / Orbiter LH2 Umbilical Disconnect Assembly
INTG 009	6	P	MPS	LOCV	SI	FC	HE	F	FE	A	c				Isolation of the ET from the Orbiter MPS or SSMEs (17 inch valve bursts open under pressure from ET)
INTG 016	12	PA	MPS	LOCV	SI	FC		P	FE	A	c		FT		Ignition Sources Igniting Flammable Fluids in the Aft Compartment
INTG 019	390	A	MPS	LOCV		FC		F	SE	A	c			ME	Premature shutdown of one or more SSME's
INTG 020	18	A	MPS	LOCV	SI	FC		P	FE	A	c		FT		Hydrogen Accumulation in the Aft Compartment During Ascent
INTG 023	20	A	MPS	LOCV	SI	FC		P	FE	A	c		FT		Contamination in the Integrated Main Propulsion System (which clogs the system)
INTG 034	24	PA	MPS	LOCV	SI	FC		P	FE	A	c			nbk	Autoignition in High Pressure Oxygen Environment (in MPS)
INTG 041	392	PA	MPS	LOCV		FC		F	FE	A	c		FT		Loss of MPS/SSME He supply pressure
INTG 042	32	PA	MPS	LOCV	SI			P	SE	A	c		FT		Turbopump Fragmentation During Engine Operation
INTG 112	48	AD	MPS	LOCV	SI	FC		P	FE	A	c		FT		H2/O2 Component Leakage During Ascent/Entry
INTG 112	49	AD	MPS	LOCV	SI	FC		P	FE	A	c		FT		H2/O2 Component Leakage During Ascent/Entry
INTG 168	81	PA	MPS	LOCV	SI	FC			EE	A	c		FT		Flammable Atmosphere in the ET Intertank (see 238)
ORBI 035	102	AD	MPS	LOCV	SI	FC		P	FE	A	c			Abt	Hydrogen Accumulation in the Orbiter Compartments During RTLS/TAL Abort
ORBI 045	107	PAOD	MPS	LOCV	SI	FC	HE	P	FE	A	c		FT		Ignition of Orbiter Fluids Entrapped in the TCS Materials (aft compartment)
ORBI 108	133	PAOD	MPS	LOCV	SI			P	SE	A	c		FT		Overpressurization of the Orbiter Aft Fuselage Caused by the Failure of an MPS Helium Regulator or Relief Valve
ORBI 278	187	PAOD	MPS	LOCV	SI			P	SE	A	c		FT		Loss of Structural Integrity Due to Overpressurization of the Mid and/or Aft Fuselage
ORBI 306	205	PA	MPS	LOCV	SI	FC		P	FE	A	c		FT		Fire/Explosion in the Orbiter Aft Compartment Caused by MPS Propellant Leakage / Component Rupture
ORBI 338	219	PA	MPS	LOCV	SI	FC		P	FE	A	c		FT		GO2 External Tank Pressurization Line as MPS/APU Ignition Source
ORBI 343	224	PA	MPS	LOCV	SI	FC		P	FE	A	c		FT		Fire/Explosion in the Orbiter Aft Compartment Caused by Contamination in the Main Propulsion System Feed System
INTG 085	44	P	MPS	LOCV	SI			P	FE	A	d		FT		Ignition of Flammable Atmosphere at T-0 Umbilicals
INTG 089	45	PA	MPS	LOCV	SI			F	SE	A	d		FT		Malfunction of the LH2 and LO2 T-0 Umbilical Carrier Plate Resulting in Damage to Shuttle Vehicle
INTG 153	71	P	MPS	LOCV	SI			P	EE	A	d			Abt	Potential Geysering in the LO2 Feed Line (Tsat = boiling point)
INTG 166	79	P	MPS	LOCV	SI	FC		P	SE	A	d			Abt	Premature Separation of Orbiter T-0 Umbilical Carrier Plate
INTG 167	80	P	MPS	LOCV	SI	FC		P	SE	A	d			Abt	Overpressurization of LO2 Orbiter Bleed System or LH2 Recirculation System
ME-FG3P	346	PA	MPS	LOCV	SI			P	SE	A	d		FT		geysering of LOX (MPS) (see 71)
ME-FG6S	354	P	MPS	LOCV	SI			P	SE	A	d			Abt	abnormal thrust loads
ME-FG8M	356	A	MPS	LOCV	SI			P	SE	A	d		FT		thrust oscillations leading to pogo (see 3)
ORBI 248	172	PAOD	MPS	LOCV	SI	FC		P	FE	A	d		FT		Fire/Explosion in GOX Pressurization System
ME-FA1S	310	P	MPS		SI	FC			FE	C	c				hydrogen fire/explosion external to aft compartment (see 21)

F. Hsu

Example Accident Initiator Bins (Hazard Categories) Developed from IMLD

(There can be a logic mapping between PRA model elements and each of the Hazard categories identified)

	Phenomnelogical Initiating Event	Hazard# Identified in IMLD
Bin-1:	Fire/explosion from external leakage/rupture	
	Ignition at ET/Orb Umbilical	INTG 006
	Ignition Sources in Aft Compt*	INTG 016
	Hydrogen Accumulation in Aft**	INTG 020
	Ingnition at T-0 Umbilical	INTG 085
	H2/O2 Leakage during Ascent	INTG 112
	H2/O2 Leakage at ET Intertank	INTG 168
	External H2 Leakage	ME FA1S
	H2 in Aft during RTLS/TAL	ORBI 035
	H2/O2 in Aft**	ORBI 306
	GO2 Press Line as Ignition Source*	ORBI 338
Bin-2:	Contamination of LH2/LO2 Systems	
	Contamination of LH2/LO2 Systems	INTG 023
	Fire/Explosion due to Contam. in LH2/LO2 Systems	ORBI 343
Bin-3:	System Overpressurization	
	Overpress of LO2 Bleed/LH2 Recirc System	INTG 167
	ET Overpressurization	P.01
	MPS H2/O2 manifold overpressure	???
	MPS propellant line overpressrization	INTG167
Bin-4:	Aft Overpressurization	
	Aft-overpress due to 750 Reg/850 RV	ORBI 108
	Generic Mid/Aft Compartment Overpressurization	ORBI 278
Bin-5:	GO2 Autoignition	
	GO2 Autoignition	INTG 034
	Ignition of fluids caught in TCS	ORBI 045
	GO2 Autoignition	ORBI 248
Bin-6:	LO2 Water-Hammer	
	GO2 Geyser during Loading/Detank	INTG 153
	GO2 Geyser during Loading/Detank	ME FG3P, A
	Functional Initiating Event	**Hazard# Identified in IMLD**
Bin-7:	Structural Failure of Umbilicals	
	Isolation of ET from Orb/SSME/Ground	INTG 009
	Physical Malfunction of T-0 Umbilical	INTG 089
	ET GH2/GO2 pressure not maintained	ORBI338, S.05
	ET Separation Failure (premature Sep. & ORB ET recontact)	ORBI289, INTG051, P.07
	MPS O2 prevalve fails to close at MECO	INTG039
Bin-8:	Loss of SSME NPSP	
	Loss of LO2 NPSP @ MECO	INTG 039
	MPS failure to maintain propellant supply to SSME	???
Bin-9:	Loss of GHe	
	Loss of GHe Supply Press	INTG 041/ORBI108
	Loss of GHe for SSME Intermediate Seal Purge	?
Bin-10:	LO2 Pogo	
	SSME Pogo	ME FG8M

F. Hsu

The "Double-T" S&MA Management Framework – Key Elements (Cont'd)

Proposed Hazard Analysis Worksheet Format

Hazard Title: **Control_Status:** **Hazard Category:**

Hazard_No: **Hazard risk index:** **Severity Class:**

Element: **Date:** 1/13/04

System: **Analyst:** F. Hsu

Subsystem: **Phase:** **Doc.#** XXX-YY

Hazard & Control #	Hazard Description	Cause factors	Potential Effects	Hazard risk index	PRA Coverage (IE/BE/Model)	Control Recom'd	Effect of Recm'd	Verifica -tion of control	Status of control
		A							
INTG37		B							
		C							

Space Shuttle Program

F. Hsu

NASA

The "Double-T" S&MA Management Framework – Key Elements (Cont'd)

Proposed Hazard Risk Assessment Matrix & Semi-quantitative Risk Index

Hazard Title& Hazard/Control No. *INTG 037* **# Causes:** *A,B,C,D,E,F* **Total Hazard Risk Index:** 2.1E-5 **Severity:** *high*

Hazard Category Frequency Bins (per mission) *(Ef =10 for each bin)*		Most Likely Effect (Risk Severity Index) - Based on worst case (LOCV) conditional likelihood)			
		Negligible 1 (.001)	Marginal 2 (0.01)	Critical 3 (0.1)	Catastrophic 4 (1.0)
1E-8 ~ 1E-6 50th: 1E-7	(1) Extremely unlikely < 1E-6	1E-10	1E-9	1E-8	1E-7
1E-6 ~ 1E-4 50th: 1E-5	(2) Remote 1E-6 ~ 1E-4	1E-8	1E-7	D 1E-6	1E-5
1E-4 ~ 1E-2 50th: 1E-3	(3) Infrequent 1E-4 ~ 1E-2	1E-6	E+F 1E-5	A·B·C 1E-4	1E-3
1E-2 ~ 1E00 50th: 1E-1	(4) Probable > 1E-2	1E-4 (1/10000)	1E-3 (1/1000)	1E-2 (1/100)	1E-1 (1/10)

$HIV = \Sigma M_{i,j}$ where $M_{i,j} = \{\Sigma X_k$ if X_k is additive; ΠX_k if X_k is multiplicative$\}$ is HIV in cell $\{i,j\}$

The "Double-T" S&MA Management Framework – Key Elements (Cont'd)

(Examples To be Provided)

- Hazard Analysis Example – Use of Semi-quantitative FTA
- Hazard Analysis Example – Use of Semi-quantitative FMECA
- Hazard Ranking Example
- Example Relationship/Mapping/Control of Hazard in PRA
- Example Accident Sequence Precursor (ASP) Identif. & Analysis
- Utilization of a RAP (Reliability Assurance Program) process

F. Hsu

The “Double-T” S&MA Management Framework – Key Elements (Cont’d)

- A Proposed Reliability Assurance (RAP) Program

- Basic Elements of A RAP Process